

Application Serial No. 09/844,447

**REMARKS**

The Applicants and the undersigned thank Examiner Gurshman for his careful review of this application and especially for his time and consideration given during the telephonic interview of February 24, 2005. A summary of this telephonic interview is provided below.

Claims 1-41 have been rejected by the Examiner. Upon entry of this amendment, Claims 2, 15, and 32 have been cancelled, and Claims 1, 3-14, 16-31, and 33-41 remain pending in this application. The independent claims are Claims 1, 14, 18, 22, 26, and 31.

Consideration of the present application is respectfully requested in light of the above claim amendments to the application, the telephonic interview, and in view of the following remarks.

**Summary of Telephonic Interview of February 24, 2005**

The Applicants and the undersigned thank the Examiner for his time and consideration given during the telephonic interview of February 24, 2005. During this telephonic interview, a proposed amendment to the claims was discussed. The Applicants provided the proposed amendment to the claims in advance of the interview and in connection with an Applicant Initiated Interview Request Form submitted by the Applicants on February 14, 2005.

Examiner Gurshman provided his thoughts on the proposed changes to the claims. The Examiner stated that he did not believe that U.S. Pat. No. 6,453,345 issued in the name of Trcka et al. (hereinafter, the "Trcka reference") provided a teaching of monitoring raw computer events from a plurality of intrusion detectors. The undersigned agreed with the Examiner that the Trcka reference does not provide any discussion of tracking raw computer events from a plurality of intrusion detectors. It was also agreed that U.S. Pat. No. 6,606,744 issued in the name of Mikurak (hereinafter, the "Mikurak reference") did not process raw computer events. The only events processed by the Mikurak reference are those related to IP telephony.

It was explained to the Examiner that the fusion engine of the invention described by this application identifies relationships between two or more raw computer events by determining if the two or more raw computer events are part of a larger computer attack. The Applicants' representative discussed one embodiment of the invention as illustrated in Figure 5.

After listening to the Applicants' representative's explanation of the claimed technology, the Examiner suggested that the fusion engine be expressly recited in the claims. The Examiner

Application Serial No. 09/844,447

also suggested that the Applicants remove the recitation of "audit systems" from the claims as it was agreed that audit systems would not likely process raw computer events.

The Examiner suggested that the embodiment that uses information from the audit systems be claimed in a separate independent claim. The Applicants' appreciate this suggestion made by the Examiner. The Applicants will file independent claims that describe audit systems in future continuation applications. For the current application, the Applicants have decided to pursue claims only describing data sources that comprise intrusion detectors.

The Examiner stated that he would conduct an update search on the technology when the Applicants submit a formal amendment containing the claims as discussed during the telephonic interview.

The Applicant and the undersigned request the Examiner to review this interview summary and to approve it by writing "Interview Record OK" along with his initials and the date next to this summary in the margin as discussed in MPEP § 713.04, p. 700-202.

#### **Claim Rejections Under 35 U.S.C. § 103**

The Examiner rejected Claims 18-22 and 40 as being anticipated by the Trcka reference. See Office Action, page 2, paragraph 4. The Examiner rejected Claims 1-17, 23-39, and 41 as being obvious over the Trcka reference in view of the Mikurak reference.

The Applicant respectfully offers remarks to traverse these pending rejections. The Applicant will address each independent claim separately as the Applicant believes that each independent claim is separately patentable over the prior art of record.

#### **Independent Claim 1**

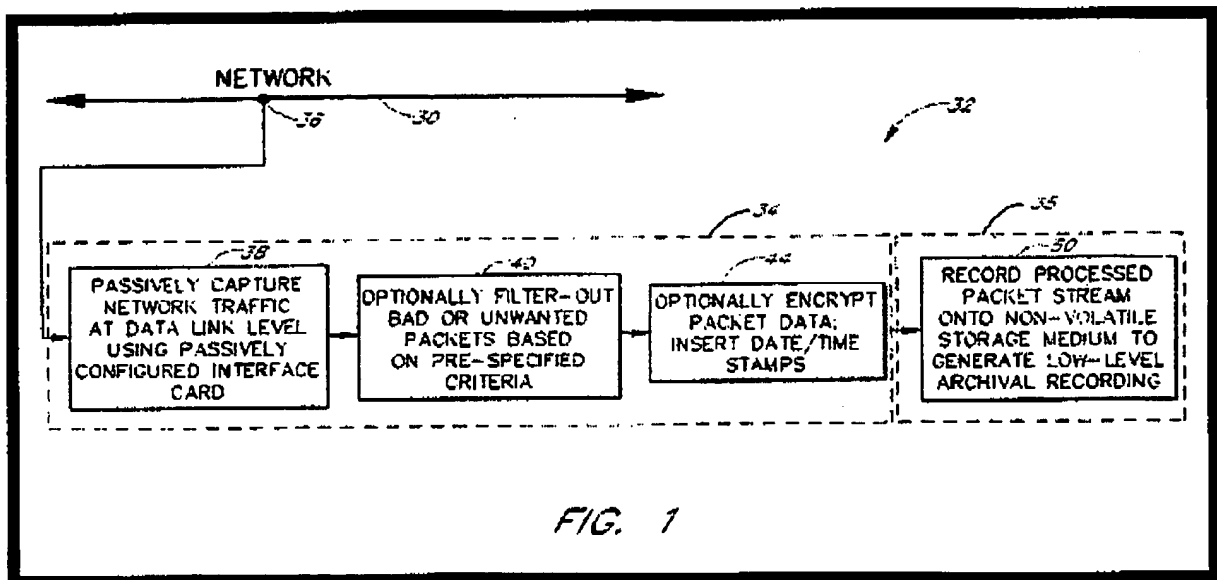
The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Trcka and Mikurak references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) receiving raw computer events with a fusion engine from one or more data sources, (2) each data source comprising an intrusion detector, (3) each raw computer event comprising one of suspicious computer activity and a computer attack; (4) classifying the raw computer events with the fusion engine; (5) storing the raw computer events; (6) assigning a ranking to each raw computer event; (7) identifying one or more relationships between two or more raw computer events with the fusion engine by (8) determining if the two or more raw

Application Serial No. 09/844,447

computer events are part of a larger computer attack; (9) in response to identifying one or more relationships between two or more raw computer events, generating a mature correlation event message; and (10) displaying one or more mature correlation event messages on one or more consoles that describe relationships between raw computer events, as recited in amended independent Claim 1.

### The Trcka Reference

The Trcka reference describes a network security and surveillance system that passively generates an archival recording of raw, bi-directional computer traffic that is present on a computer network 30 as illustrated in Figure 1 of the reference. The Trcka system includes a monitoring computer 34 that is connected to the computer network 30 at a network monitoring point 36. See Figure 1 of the Trcka system reproduced below.



The monitoring computer 34 of the Trcka reference includes an interface card 38 for passively capturing network traffic at the data link level. The monitoring computer 34 employs a filter 40 to remove bad or unwanted packets based on pre-specified criteria. After bad or unwanted packets are removed, the computer 34 has an encryption device 44 that can encrypt the packet data as well as insert date and time stamps.

Application Serial No. 09/844,447

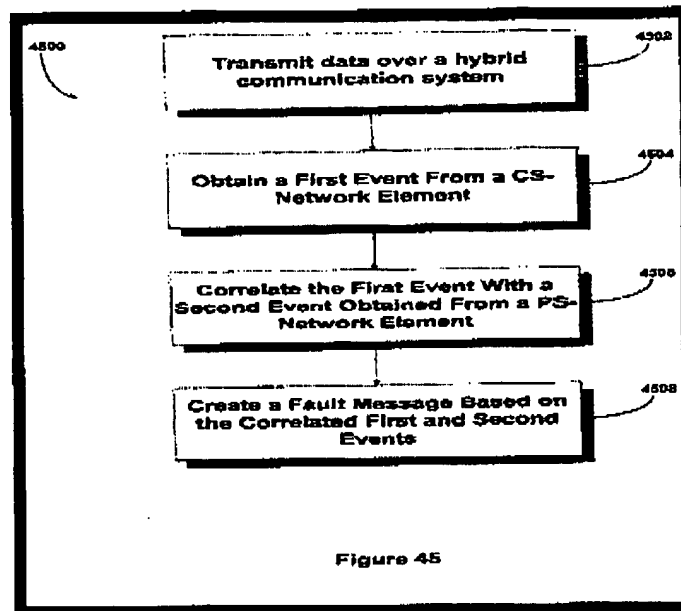
Once data and time stamps have been inserted, the computer 34 has a non-volatile storage medium 50 that can maintain a complete replica of all valid network traffic. See the Trcka reference, column 5, lines 25-45; column 6, lines 40-68; and in column 7, lines 14-42.

Opposite to the monitoring computer 34 of the Trcka reference, the invention described by amended independent Claim 1 provides the receiving of raw computer events with a fusion engine from one or more data sources wherein each data source comprises an intrusion detector and wherein each raw computer event comprises one of suspicious computer activity and a computer attack;. The fusion engine as described by amended independent Claim 1 identifies one or more relationships between two or more raw computer events by determining if the two or more raw computer events are part of a larger computer attack. The Trcka reference does not provide any teaching of monitoring raw computer events from multiple intrusion detectors and determining if two or more raw computer events are part of a larger attack, as recited in amended independent Claim 1 in combination with the other claim elements.

#### The Mikurak Reference

The Examiner admits that the Trcka reference fails to provide any teaching of generating one or more correlation event messages. To make up for this deficiency, the Examiner relies upon the Mikurak reference.

Specifically, the Examiner refers ISS to Figure 45 of the Mikurak reference to provide a teaching of a "mature correlation event message." Figure 45 of the Mikurak reference illustrates a flowchart showing a Fault Management Process. See Figure 45 of the Mikurak reference reproduced below.



Step 4508 (the last step of the flow chart reproduced above) describes a fault message based on correlated first and second events. These events are associated with a performance of packet-switched (PS) and circuit-switched (CS) telephone systems. See Mikurak reference, column 70, line 50 through column 71, line 22.

The Mikurak system generally describes integrated Internet Protocol (IP) telephony services allowing a user of a web application to communicate in an audio fashion in-band without having to pick up another telephone. Users can click a button and go to a call center through the network using IP telephony. The system invokes an IP telephony session simultaneously with the data session, and uses an active directory lookup whenever a user uses the system. See Mikurak reference, column 2, lines 60-68.

The Mikurak-Trcka combination proposed by the Examiner does not provide any teaching of receiving of raw computer events with a fusion engine from one or more data sources wherein each data source comprises an intrusion detector and wherein each raw computer event comprises one of suspicious computer activity and a computer attack. The fusion engine as described by amended independent Claim 1 identifies relationships between two or more raw computer events by determining if the two or more raw computer events are part of a larger computer attack. Like the Trcka reference, the Mikurak reference does not provide any teaching of monitoring raw computer events from multiple intrusion detectors and determining if two or more raw computer events are part of a larger attack, as recited in amended independent Claim 1.

Application Serial No. 09/844,447

Conclusion Regarding Independent Claim 1

In light of the differences between Claim 1 and the Trcka and Mikurak references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of this rejection of Claim 1 are respectfully requested.

Independent Claim 14

The rejection of Claim 14 is respectfully traversed. It is respectfully submitted that the Trcka and Mikurak references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) receiving a plurality of raw computer events with a fusion engine from one or more intrusion detectors, (2) each raw computer event having a first set of parameters and comprising one of suspicious computer activity and a computer attack; (3) creating raw computer event storage areas based upon information received from a raw computer event classification database; (4) storing each event in an event storage area based upon an event type parameter; (5) comparing each raw computer event to data contained in a context database with the fusion engine to determine if the two or more raw computer events are part of a larger computer attack; (6) adjusting a priority parameter or leaving the priority parameter in tact for each raw computer event in response to the comparison to the context database; (7) associating each raw computer event with one or more correlation events; (8) applying one or more rules to each raw computer event based upon the correlation event associations; and (9) generating a mature correlation event message in response to each successful application of a rule, as recited in amended independent Claim 14.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address a combination of elements comprising: receiving a plurality of raw computer events with a fusion engine from one or more intrusion detectors, as recited in amended independent Claim 14.

In light of the differences between Claim 14 and the Trcka and Mikurak references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent

Application Serial No. 09/844,447

Claim 14. Accordingly, reconsideration and withdrawal of this rejection of Claim 14 are respectfully requested.

Independent Claim 18

The rejection of Claim 18 is respectfully traversed. It is respectfully submitted that the Trcka and Mikurak references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) a plurality of data sources comprising intrusion detectors; (2) an event collector linked to the plurality of data sources; (3) a fusion engine linked to the event collector, (4) the fusion engine identifying relationships between two or more raw computer events generated by the data sources, (5) by determining if the two or more raw computer events are part of a larger computer attack, (6) each raw computer event comprising one of suspicious computer activity and a computer attack; and (7) a console linked to the event collector for displaying any output generated by the fusion engine, as recited in amended independent Claim 21.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address a combination of elements comprising: a fusion engine identifying relationships between two or more raw computer events generated by the data sources, by determining if the two or more raw computer events are part of a larger computer attack,, as recited in amended independent Claim 18.

In light of the differences between Claim 18 and the Trcka and Mikurak references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 18. Accordingly, reconsideration and withdrawal of this rejection of Claim 18 are respectfully requested.

Independent Claim 22

The rejection of Claim 22 is respectfully traversed. It is respectfully submitted that the Trcka and Mikurak references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) a controller; (2) an event reader for receiving raw computer events from intrusion detectors, (3) each raw computer event comprising one of suspicious computer activity and a computer attack; (4) a classifier linked to the event reader for classifying

Application Serial No. 09/844,447

the received raw computer events; (5) a raw computer event classification database linked to the classifier; (6) a context based risk-adjustment processor linked to the classifier, for adjusting priorities of raw computer events; (7) a context database linked to the context based risk-adjustment processor; and (8) a rule database, for identifying if one or more relationships exist between two or more events by determining if the two or more raw computer events are part of a larger computer attack, as recited in amended independent Claim 22.

Similar to the analysis independent Claim 1, neither the Trcka nor the Mikurak references alone or in combination teach an event reader for receiving raw computer events from intrusion detectors, wherein each raw computer event comprising one of suspicious computer activity and a computer attack, and identifying if one or more relationships exist between two or more events by determining if the two or more raw computer events are part of a larger computer attack.

In light of the differences between Claim 22 and the Trcka and Mikurak references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 22. Accordingly, reconsideration and withdrawal of this rejection of Claim 22 are respectfully requested.

#### Independent Claim 26

The rejection of Claim 26 is respectfully traversed. It is respectfully submitted that the Trcka and Mikurak references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) receiving with a fusion engine a raw computer event having a first ranking from one or more data sources comprising intrusion detectors, (2) each raw computer event comprising one of suspicious computer activity and a computer attack; (3) classifying the raw computer event with the fusion engine; (4) storing the raw computer event; and (5) assigning a second ranking to the raw computer event with the fusion engine, whereby (6) the second ranking assesses risks of the raw computer event based upon a context of the raw computer event and (7) indicates if the raw computer event is part of a larger computer attack, as recited in amended independent Claim 26.

Similar to the analysis independent Claim 1, neither the Trcka nor the Mikurak references alone or in combination teach receiving with a fusion engine a raw computer event having a first ranking from one or more data sources comprising intrusion detectors, each raw computer event



Application Serial No. 09/844,447

comprising one of suspicious computer activity and a computer attack, and indicating if the raw computer event is part of a larger computer attack.

In light of the differences between Claim 26 and the Trcka and Mikurak references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 26. Accordingly, reconsideration and withdrawal of this rejection of Claim 26 are respectfully requested.

Independent Claim 31

The rejection of Claim 31 is respectfully traversed. It is respectfully submitted that the Trcka and Mikurak references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) receiving raw computer events with a fusion engine from one or more data sources comprising intrusion detectors, (2) each raw computer event comprising one of suspicious computer activity and a computer attack; (3) classifying the raw computer events with the fusion engine; (4) grouping two or more raw computer events into a high level correlation event with the fusion engine if the two or more raw computer events are part of a larger computer attack; (5) in response to grouping the two or more raw computer events, generating a mature correlation event message; and (6) displaying one or more mature correlation event messages on a console that describe relationships between raw computer events, whereby a number of events displayed on the console are substantially minimized, as recited in amended independent Claim 31.

Similar to the analysis independent Claim 1, neither the Trcka nor the Mikurak references alone or in combination teach receiving with a fusion engine a raw computer event from one or more data sources comprising intrusion detectors, each raw computer event comprising one of suspicious computer activity and a computer attack, and indicating if the raw computer event is part of a larger computer attack.

In light of the differences between Claim 31 and the Trcka and Mikurak references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 31. Accordingly, reconsideration and withdrawal of this rejection of Claim 31 are respectfully requested.

Application Serial No. 09/844,447

Dependent Claims 3-13, 16-17, 19-21, 23-25, 27-30, and 33-41

The Applicant respectfully submits that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references. The Applicant also respectfully submits that the recitations of these dependent claims are of patentable significance.

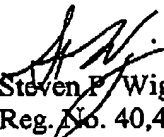
In view of the foregoing, the Applicant respectfully requests that the Examiner withdraw the pending rejections of dependent Claims 3-13, 16-17, 19-21, 23-25, 27-30, and 33-41.

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on November 19, 2004. The Applicants and the undersigned thank Examiner Gurshman for consideration of these remarks. The Applicants have amended the claims and have submitted remarks to traverse rejections of Claims 1-41. The Applicants respectfully submit that the present application is in condition for allowance. Such action is hereby courteously solicited.

If the Examiner believes that there are any issues that can be resolved by a telephone conference, or that there are any formalities that can be corrected by an Examiner's amendment, the Examiner is invited to contact the undersigned in the Atlanta Metropolitan area (404) 572-2884.

Respectfully submitted,

  
Steven P. Wigmore  
Reg. No. 40,447

King & Spalding LLP  
191 Peachtree Street, N.E.  
Atlanta, Georgia 30303-1763  
telephone: (404) 572.4600  
K&S File No. 05456-105006